CLAIMS

We claim:

1. Method for the management of certificates stored on an identity module, said method comprising:

providing an identity module comprising a data processing device, a storage device connected to said data processing device, a card certificate stored on the storage device, an application which uses the certificates stored on the identity module, and a data transfer device which is connected to said data processing device and which is provided with a communication interface for the transfer of information between an external device and the identity module,

receiving a certificate to the identity module;

authenticating said certificate by means of said card certificate; and

storing information obtained from said authenticated certificate on said storage device.

2. Method according to claim 1, further comprising filtering said authenticated certificate to remove a certification chain contained in said authenticated certificate.

3. Method according to claim 1, wherein said certificate is authenticated by means of the card certificate before its use.

4. Method according to claim 1, wherein said stored information comprises a public key and an associated identity.

5. Method according to claim 1, further comprising verifying whether said certificate is authentic prior to storage, and when authenticity cannot be verified, rejecting said certificate.

6. Method according to claim 1, further comprising verifying whether said certificate is authentic before its use, and when authenticity cannot be verified, rejecting said certificate.

7. Method according to claim 2, wherein the filtering comprises verifying whether each signature in said certificate is authentic, and filtering out only signatures that the verification proves to be authentic.

8. Identity module for the management of certificates, said identity module comprising:

a data processing device;

a storage device connected to said data processing device;

a card certificate stored on the storage device;

an application which uses certificates;

a data transfer device, which is connected to said data processing device and which is provided with a communication interface for the transfer of information between an external device and the identity module;

means for receiving a certificate to the identity module;

means for authenticating said certificate by means of said card certificate; and

means for storing information contained in said authenticated certificate on said storage device.

9. Identity module according to claim 8, wherein the identity module further comprises:

means for filtering out from the certificate a certification chain contained in said authenticated certificate.

10. Identity module according to claim 8, wherein the identity module further comprises means for establishing the authenticity of said certificate by means of a card certificate before its use.

11. Identity module according to claim 8, wherein the identity module further comprises:

means for verifying whether said certificate is authentic prior to storage indicates that it its unreliable; and

means for rejecting said certificate when authenticity cannot be verified.

12. Identity module according to claim 8, wherein the identity module further comprises:

means for verifying whether said certificate is authentic prior to use; and

means for rejecting said certificate when authenticity cannot be verified.

13. Identity module according to claim 9, wherein the identity module further comprises means for verifying the authenticity of each signature contained in said certificate before filtering.